

In the Claims:

Please amend claims 1, 18, 35, 36 and 38 as indicated below.

1. (Currently amended) A method of accepting a pass code, comprising:

providing a user with a machine-generated challenge; and

receiving, from a user-input device, user input ~~capable of~~ which represents a transformation[[ing]] of the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the user input ~~capable of transforming the machine-generated challenge into the pass code~~ is different for different machine-generated challenges;

generating a response from the user input received from the user input device, wherein the user input does not include the pass code itself; and

transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting, wherein said response allows[[ing]] the user to be validated at the remote authorisation unit dependent on said response compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code.

2. (Original) The method of claim 1, wherein said challenge is independent of said pass code.

3. (Original) The method of claim 1, further comprising generating a new challenge for each user validation.

4. (Original) The method of claim 3, wherein said challenge is generated on a random basis.

5. (Original) The method of claim 3, wherein the challenge is generated in response to receiving a request from a user for validation.

6. (Original) The method of claim 1, wherein providing a user with a challenge comprises displaying the challenge to the user.

7. (Original) The method of claim 6, wherein the challenge is displayed to the user in such a manner as to prevent third parties from viewing the challenge.

8. (Previously presented) The method of claim 1, wherein the user input from the user-input device is received as a set of one or more modifications to be applied to the challenge so that it matches the pass code allocated to the user.

9. (Original) The method of claim 8, wherein said set of one or more modifications is received as directional input from the user.

10. (Original) The method of claim 9, wherein said directional input is received as the result of the user pressing one or more arrow keys that increment or decrement the challenge by a fixed amount.

11. (Original) The method of claim 1, wherein said challenge has the same number of characters as the pass code allocated to the user.

12. (Original) The method of claim 11, wherein said transformation is specified individually for each character of the challenge.

13. (Original) The method of claim 12, further comprising receiving an indication from the user that the transformation for a different character is about to be entered.

14. (Previously presented) The method of claim 1, further comprising receiving an indication from the user that the user input to transform the challenge has been completely entered.

15. (Previously presented) The method of claim 1, further comprising generating a pass code from the challenge and from the response.

16. (Previously presented) The method of claim 15, wherein the response is validated by comparing the generated pass code with the stored data record of the pass code.

17. (Previously presented) The method of claim 1, further comprising:

receiving a communications challenge from the remote authorisation unit that has access to said stored data record of the pass code;

using the response to encrypt said communications challenge; and

transmitting the encrypted communications challenge to the remote authorisation unit;

thereby allowing the response to be validated by said remote authorisation unit using said stored data record of, the pass code.

18. (Currently amended) A terminal for use in accepting a pass code, comprising:

an output for providing a user with a machine-generated challenge; and

a user-input device for receiving user input ~~capable of~~ which represents a transformation[[ing]] of the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the user input ~~capable of transforming the machine-generated challenge into the pass code~~ is different for different machine-generated challenges;

wherein said terminal is further configured to:

generate a response from the user input received from the user input device, wherein the user input does not include the pass code itself;
and

transmit the response to a remote authorisation unit to authenticate the response, wherein the response is transmitted without the pass code and without the terminal generating the pass code from the response prior to transmitting, wherein said response allows[[ing]] the user to be validated at the remote authorisation unit dependent on said response compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code.

19. (Original) The terminal of claim 18, wherein said challenge is independent of said pass code.

20. (Original) The terminal of claim 18, wherein a new challenge is generated for each user validation.

21. (Original) The terminal of claim 20, wherein said challenge is generated on a random basis.

22. (Original) The terminal of claim 20, wherein the challenge is generated in response to receiving a request from a user for validation.

23. (Original) The terminal of claim 18, further comprising a display, wherein the challenge is provided to the user on the display.

24. (Original) The terminal of claim 23, wherein the terminal is configured to prevent parties other than the user from viewing the challenge on the display.

25. (Previously presented) The terminal of claim 18, wherein the user input from the user-input device is received as a set of one or more modifications to be applied to the challenge so that it matches the pass code allocated to the user.

26. (Original) The terminal of claim 25, wherein said set of one or more modifications is received as directional input from the user.

27. (Previously presented) The terminal of claim 26, wherein the user-input device comprises one or more arrow keys that increment or decrement the challenge by a fixed amount.

28. (Original) The terminal of claim 18, wherein said challenge has the same number of characters as the pass code allocated to the user.

29. (Original) The terminal of claim 28, wherein said transformation is specified individually for each character of the challenge.

30. (Previously presented) The terminal of claim 29, wherein the user-input device comprises a key for receiving an indication from the user that the transformation for a different character is about to be entered.

31. (Previously presented) The terminal of claim 18, wherein the user-input device comprises a key for receiving an indication from the user that the user input to transform the challenge has been completely entered.

32. (Previously presented) The terminal of claim 18, wherein the pass code is generated from the challenge and from the user input from the user-input device.

33. (Previously presented) The terminal of claim 32, wherein the user is validated by comparing the generated pass code with a stored data record of the pass code.

34. (Previously presented) The terminal of claim 18, further comprising a communications link with the remote authorisation unit that has access to a stored data record of the pass code, wherein the terminal receives a communications challenge from said remote authorisation unit and uses a response generated from the user input to encrypt said communications challenge, and wherein the encrypted communications challenge is transmitted to the remote authorisation unit, thereby allowing the response to be validated by said remote authorisation unit against said stored data record of the pass code.

35. (Currently amended) An apparatus, comprising:

means for providing a user with a machine-generated challenge;

means for receiving user input ~~capable of~~ which represents a transformation[[ing]]
of the machine-generated challenge into a pass code allocated to the user,
wherein the user input is dependent on the machine-generated challenge

such that the user input ~~capable of transforming the machine-generated challenge into the pass code~~ is different for different machine-generated challenges;

means for generating a response from the user input received from the user input device, wherein the user input does not include the pass code itself;
and[[;]]

means for transmitting the response to a remote authorisation unit to authenticate the response without transmitting the pass code to the remote authorisation unit and without generating the pass code from the user input prior to said transmitting.

36. (Currently amended) A method for using a pass code to validate a user, comprising:

receiving a request from a user for validation;

generating a challenge in response to said request;

providing the user with the challenge;

receiving, from a user-input device, user input ~~capable of~~ which represents a transformation[[ing]] of the challenge into a pass code allocated to the user, wherein the user input is dependent on the challenge such that the user input ~~capable of transforming the challenge into the pass code~~ is different for different challenges;

generating a response from the user input received from the user input device, wherein the response is not the pass code, and wherein the user input does not include the pass code itself;

generating a predicted response based on knowledge of the challenge and a stored version of the pass code; and

validating the user on the basis of said response compared to the predicted response, wherein neither the response nor the predicted response is the pass code.

37. (Canceled)

38. (Currently amended) A computer program product comprising instructions encoded on a storage medium, said instructions when loaded into a machine causing the machine:

to provide a user with a machine-generated challenge; and

receive, from a user-input device, user input ~~capable of~~ which represents a transformation^{[[ing]]} of the machine-generated challenge into a pass code allocated to the user, wherein the user input is dependent on the machine-generated challenge such that the user input ~~capable of transforming the machine-generated challenge into the pass code~~ is different for different machine-generated challenges;

generate a response to the challenge from the user input received from the user input device, wherein the user input does not include the pass code itself; and

transmitting the response to a remote authorisation unit to authenticate the response, without transmitting the pass code to the remote authorization unit and without generating the pass code from the response prior to said transmitting, wherein said response allows^{[[ing]]} the user to be validated

at the remote authorisation unit dependent on said response compared to a predicted response based on knowledge of the challenge and a stored data record of the pass code.

39. (Original) The computer program product of claim 38, wherein said challenge is independent of said pass code.

40. (Original) The computer program product of claim 38, wherein said instructions further cause the machine to generate a new challenge for each user validation.

41. (Original) The computer program product of claim 40, wherein the challenge is generated in response to receiving a request from a user for validation.

42. (Original) The of computer program product of claim 40, wherein said challenge is generated on a random basis.

43. (Original) The computer program product of claim 38, wherein providing a user with a challenge comprises displaying the challenge to the user.

44. (Original) The computer program product of claim 43, wherein the challenge is displayed to the user in such a manner as to prevent third parties from viewing the challenge.

45. (Previously presented) The computer program product of claim 38, wherein the user input from the user-input device is received as a set of one or more modifications to be applied to the challenge so that it matches the pass code allocated to the user.

46. (Original) The computer program product of claim 45, wherein said set of one or more modifications is received as directional input from the user.

47. (Original) The computer program product of claim 46, wherein said directional input is received as the result of the user pressing one or more arrow keys that increment or decrement the challenge by a fixed amount.

48. (Original) The computer program product of claim 38, wherein said challenge has the same number of characters as the pass code allocated to the user.

49. (Original) The computer program product of claim 48, wherein said transformation is specified individually for each character of the challenge.

50. (Previously presented) The computer program product of claim 49, wherein said instructions further cause the machine to receive an indication from the user-input device that the transformation for a different character is about to be entered.

51. (Previously presented) The computer program product of claim 38, wherein said instructions further cause the machine to receive an indication from the user that the user input to transform the challenge has been completely entered.

52. (Previously presented) The computer program product of claim 38, wherein said instructions further cause the machine to generate the pass code from the challenge and from the user input from the user-input device.

53. (Canceled)

54. (Previously presented) The computer program product of claim 38, wherein the instructions further cause the machine:

to receive a communications challenge from the remote authorisation unit that has access to a stored data record of the pass code;

to use the a response generated from the user input to encrypt said communications challenge; and

to transmit the encrypted communications challenge to the remote authorisation unit, thereby allowing the response to be validated by said remote authorisation unit using said stored data record of the pass code.